REPERCUSIÓN EN EL MUNDO

Cotizan al alza. El ataque masivo del virus malicioso WannaCry ha provocado la inmediata reacción alcista en la Bolsa de Nueva York de los valores relacionados con ciberseguridad. Las acciones del fabricante Palo Alto Networks se anotaron un repunte del 4,25 %.

Previsibles. La Red Nacional de Investigación en Ciberseguridad (Renic) destacó ayer que la situación creada por el ciberataque mundial era "previsible" y que ya se había advertido sobre la dependencia de las empresas españolas de las TIC.

Recaudación. Más de 300.000 computadoras en 150 países resultaron infectadas desde el viernes por el ciberataque global, pero sus responsables recaudaron menos de 70.000 dólares (63.774 euros) con su chantaje a los afectados.

***Hacker* ético.** Rod Soto, secretario de Hack Miami, una comunidad de *hackers* éticos" del sur de Florida, declaró a Efe que no duda de que Rusia es "parcialmente responsable" del ciberataque con fines extorsivos que dejó más de 200.000 afectados.

Mayor seguridad. Asia sufrió ayer nuevos estragos por el ciberataque mundial en medio de las recomendaciones de los expertos para que se refuerce la seguridad y el anuncio de China sobre una nueva versión del virus, que ya afecta a 30.000 empresas.

EMPRESA AFECTADA

Belén Bermúdez

Administradora de Comercial Moncho-Pontecesures

"NOS SALVÓ EL TENER COPIAS DE SEGURIDAD"

Comercial Moncho S.L., una empresa de ferretería, materiales de construcción y muebles de Pontecesures fue una de las firmas que sufrieron el ataque del ransomware WannaCry el pasado viernes. Belén Bermúdez es una de sus administradoras y lo primero que dice es que "no pagamos nada. Tendremos que pagar a nuestra empresa informática pero a los que lo hicieron... nada de nada".

¿Qué ocurrió?

Abrimos como todos los días sobre las nueve y cuando fuimos a encender los ordenadores no arrancaban con normalidad y comprobamos que en la pantalla había un mensaje no habitual y sospechoso en inglés.

¿Qué hicieron en la empresa?

Hablé con mi hermano Álvaro, que es el que controla el sistema y él se puso en contacto con nuestra empresa de Informática y sus técnicos ya nos avisaron de que apagáramos todos los equipos y no tocáramos nada.

¿Y cómo actuaron ellos?

Llegó un informático y trató de solucionarlo pero no lo pudo conseguir por lo que decidieron llevarse los servidores. En 24 lograron reactivar todo tras contrarrestar el virus invasivo.

¿Recuperaron la información o los sistemas operativos?

En nuestra empresa tenemos la obligación de hacer copias de seguridad y por eso salvamos todo. La última se había hecho tras cerrar el jueves y como el ataque se produjo durante la madrugada no perdimos nada. ¡¡Si se hubiera producido a lo largo de la jornada sí que hubiera sido un desastre!!

¿Qué problemas tuvieron?

Durante todo el viernes y la mañana del sábado nos vimos obligados a trabajar a la antigua usanza; es decir, cobrando manualmente, sin poder consultar ni precios ni catálogos, sin albaranes ni facturas. Tuvimos que ir improvisando sobre la marcha ya que toda la información está en los ordenadores y no teníamos acceso a ellos.

¿Tenían filtros de seguridad?

Los antivirus habituales y nunca antes habíamos tenido problemas. Ahora pusimos nuevos filtros.

¿Qué enseñanza se puede sacar?

Lo más importante es que nos salvo tener copias de seguridad y habrá que seguir haciéndolas tres veces al día.

INGENIERO INFORMÁTICO

Fernando Suárez Lorenzo

Presidente del Colexio Profesional de Enxeñaría en Informática de Galicia

"ES LA PUNTA DEL ICEBERG DE TODO LO QUE ESTÁ POR VENIR"

El presidente del Colexio de Enxeñaría en Informática de Galicia (CPEIG), el ferrolano Fernando Suárez, tiene muy claro que "este ataque es el primero de muchos, es la punta del iceberg de todo lo que está por venir". Porque, de hecho, ataques globales de este tipo pueden nacer de las mentes de "mafias, organizaciones" e incluso "gobiernos".

Es muy difícil que una empresa dé la cara y confiese que es una víctima..

Sí, porque se produce una merma de la confianza. Sería una campaña de *marketing* muy negativa para las empresas, Por lo menos en nuestro país, se vio que el impacto fue menor de lo esperado. Este es un ataque muy visible. Se sabe si estás o no infectado. El problema real es que vulnerabilidades como estas pueden explotar para robar datos y no trasciende. Galicia sufre, según Incibe, más de 2.000 ataques al día y no se perciben.

Además, no hay ningún tipo de obligatoriedad legal de publicar incidentes de este estilo. Porque, además, el activo más importante de cualquier empresa es la información.

¿Qué precio hay que pagar por este secuestro cibernético?

Tiene consecuencias económicas, pero hay que valorar el esfuerzo de tiempo que supone recuperarla, aun teniendo copias de seguridad. Por eso a veces las empresas optan por pagar un rescate.

¿Existe algún punto positivo?

Lo positivo es que las empresas de seguridad están incrementando sus ventas porque se genera concienciación de la necesidad de invertir en seguridad, se genera también concienciación a nivel social de ciertas pautas de conducta que son peligrosas, como abrir archivos y correos de remitentes desconocidos o incluso no tener aplicaciones actualizadas o no disponer de *software* antivirus.

Apuntaba hace unos días en este periódico que los conflictos entre países se están trasladando cada vez más al ámbito cibernético.

Sí, por eso es necesario contar con sistemas, con profesionales y con equipos organizados.

Entonces, ¿qué me dice de la propuesta de reclutar *hackers* civiles?

Desconozco su contenido, pero lo lógico sería profesionalizar, tener un ciberejército muy formado, muy actualizado que compartiese ese conocimiento con otras potencias y que realmente estuviésemos seguros, y no delegar, en cierto modo, la seguridad de infraestructuras críticas en esas *milicias* de desconocidos, en muchos casos, y que tampoco ofrecen una garantía de continuidad. Eso es muy necesario y desde los colegios reclamamos la regulación de la profesión y que los gobiernos inviertan en profesionales competentes y formados.

¿Qué nivel tiene Galicia?

Galicia se podría erigir un polo de conocimiento específico en el ámbito de la ciberseguridad, ya que existen empresas que están dando servicio dentro y fuera de la comunidad. Por ejemplo: Tarlogic, Improsec o Emetel. M. ALMODÓVAR

SECTOR TIC DE GALICIA

Lucía Gregorio

Directora general del colectivo de empresas TIC gallegas INEO

"SE DEBE BLINDAR EL SERVICIO PÚBLICO Y DATOS DE USUARIOS"

Desde esta asociación, referente asociativo empresarial del sector TIC en Galicia, su directora detalla que "en este tipo de ataques el punto de entrada más vulnerable es el usuario que abre lo que no debe". Por eso receta "un buen plan de seguridad en la empresa, es básico".

¿Cómo evitamos que pase algo así?

Hay que tener un protocolo claro de ciberseguridad y que lo siga toda la plantilla. Desde no usar correos personales en dispositivos de trabajo, a no introducir USBs ni conectar dispositivos de almacenamiento externo. También hay que establecer un protocolo de copias de seguridad eficaz.

¿Qué ámbitos hay que blindar?

Los puntos principales suelen ser infraestructuras básicas: redes eléctricas, conectadas ahora en su mayoría, con muchos datos de clientes que 'secuestrar'; telefonía; bancos y aseguradoras.... Pero como el fin es encriptar información para pedir un rescate por el descifrado cualquier ámbito que maneje muchos datos de usuarios y que pueda provocar disfunciones en el servicio son objetivos prioritarios, de ahí que atacasen a sistemas de salud.

EMPRESA DE SEGURIDAD

Rafael Villaverde

Propietario y administrador (CEO) de Infonet

"SI NO SE TOMARON MEDIDAS NO QUEDA OTRA: PAGA"

La compostelana Infonet es un referente en ciberseguridad, interna y externa. Su líder alega que, pese al estigma que pueda suponer, "el nuevo reglamento de protección de datos obliga a las empresas a comunicar a las autoridades de control, y en casos graves a los afectadas –clientes y proveedores– en un máximo de 72 horas que hemos sufrido un ciberataque".

¿Han detectado gran impacto?

Numerosos clientes este fin de semana nos preguntaban si estaban en riesgo, si el virus podría transmitirse a través de la red de Telefónica por el mero hecho de ser abonados, y preguntando si debían apagarlo todo. ¡Que no cunda el pánico! Esta amenaza es tan sólo una más de las que desde 2014 ya existen, sólo que más sofisticada: la vía de entrada es el correo electrónico, no abrir nunca uno sospechoso.

¿Saben de contagios?

Hace una semana un cliente del sector sanitario se infectaba con una variante similar al WannaCry, y llegaba el caos: imposibilidad de dar citas, historiales médicos inaccesibles, máquinas de resonancia inutilizadas, toda la organización afectada y paralizada... lo primero era aislar el equipo infectado. El disponer de copias de seguridad permitió volver a la normalidad a las pocas horas, sin daños colaterales y sin poner en riesgo la organización.

¿Y de no haber copias?

La triste realidad es que la mayor parte de las empresas no tienen una adecuada política de copias de seguridad. Sin ellas, de resultar infectado recomendamos pagar a los secuestradores.

¿Pagar? Eso va contracorriente...

Si, pagar, nadie lo está recomendando, pero entre no fomentar el cibercrimen y perder la información de nuestra empresa o nuestros clientes, poniendo en peligro la viabilidad de nuestro negocio, no lo dude, pague.

¿Saben de casos?

A una gestoría se lo cifraron todo, facturas, contabilidad de clientes, impuestos... Pensaba que tenía copias de seguridad, pero hacía un año que no. Tuvo que pagar. Primero le pidieron un bitcoin (900 €)... y cuando lo pagó le reclamaron otros dos. Entonces le enviaron la herramienta de descifrado. El encriptado se produjo en pocas horas. Para deshacerlo, dos días.